

Kybernetická bezpečnost obcí

v kontextu směrnice NIS2

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

28. Března 2023
TLP: CLEAR

Jan Hénik
oddělení regulace veřejného sektoru



- Směrnice NIS2 byla dne 27. prosince 2022 zveřejněna v Úředním věstníku Evropské unie. Publikovaná podoba směrnice NIS2 je oficiální a nebude se již dále měnit.
- Informace v této prezentaci vycházejí z finálního znění směrnice.
- Prezentované informace týkající se budoucí úpravy právních předpisů České republiky v závislosti na obsahu směrnice NIS2 mohou obsahovat názory a plány NÚKIB jako gestora této problematiky.
- Prezentace má informační a osvětových charakter a vychází z aktuálního stavu poznání.



- Směrnice obecně je legislativní akt Evropské unie, který není* sám o sobě aplikovatelný (= **musí nejdříve vzniknout národní úprava**)
- Kybernetická bezpečnost v České republice **je již nyní regulována** (= je z čeho vycházet)
- Základem změn je nově přicházející **směrnice NIS2** (= viz dále), ale také potřeba zákon o kybernetické bezpečnosti aktualizovat
- Národní úřad pro kybernetickou a informační bezpečnost **připravil návrh nového zákona o kybernetické bezpečnosti** (= byl zveřejněn k připomínkám)
- NÚKIB nemůže „podkročit“ směrnici NIS2.
- Předpisy z návrhů se **budou** měnit – zveřejnili jsme je ke konzultaci, proto nyní zapracováváme vstupy a ještě tyto návrhy čeká MPŘ
 - K informacím o změnách se dostanete – NÚKIB je bude komunikovat na webu k NIS2 a poskytne rád i jejich výklad

*zpravidla



- Směrnice byla publikována 27. prosince 2022
 - Gestor problematiky (předkladatel návrhu transpozičního zákona) = NÚKIB
 - **Transpozice, tj. provedení obsahu směrnice do českého práva je potřeba provést do 17. října 2024 – nová pravidla budou platná.**
- => Návrh odejde do legislativního procesu (LRV, MPŘ, Parlament...) v polovině 2023



Směrnice NIS2 navazuje na obsah směrnice NIS1 přijaté v roce 2016 a poprvé zavádí povinnou regulaci veřejné správy ze strany členských států.

ČR měla již existující úpravu kybernetické bezpečnosti veřejné správy.

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential“.

ENERGETIKA



Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.



Subjekty poskytující službu dálkového vytápění nebo chlazení.



Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.



Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.



Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA



Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.



Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.



Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.



Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ



Sektor bankovníctví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ



Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ



Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA



Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA



Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA



Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů.

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB



Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA



Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR



V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik“ a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik“ a „střední podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important“ (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY



Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ



Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL



Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ



Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA



Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB



Poskytovatelé on-line tržišť, internetových vyhledávačů, platform služeb sociálních sítí.

VÝZKUM



Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.



- Regulace se netýká každého v daném odvětví – musí být splněna kritéria:
 - Organizace poskytuje alespoň jednu službu uvedenou v přílohách směrnice, a zároveň
 - Je středním nebo velkým podnikem, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obrátu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK)
- Počítání **velikosti** podniku – nutno zohlednit i majetkově propojené společnosti
- Vybrané služby – **všechny organizace neohledě na jejich velikost** (ISPs, poskytovatelé služeb vytvářejících důvěru, DNS, veřejná správa)
- **Dodatečná kritéria** pro subjekty působící v regulovaných odvětvích bez ohledu na jejich velikost (jediný poskytovatel, narušení služby by mohlo mít významný dopad na veřejnou bezpečnost nebo zdraví osob nebo by mohlo vyvolat významné riziko, zejména s přeshraničním dopadem)
- Propojení směrnice NIS2 s tzv. směrnicí CER – **povinná osoba podle CER** (neznámá množina) → povinná osoba podle NIS2



- Směrnice NIS2 ([EUR-Lex - 32022L2555 - CS - EUR-Lex \(europa.eu\)](#)) stanovuje široce povinné osoby, dělí je do dvou skupin (základní a významné), přiřazuje jim různé povinnosti (bezpečnostní opatření, hlášení incidentů,...)
 - = **stanovuje minimum**, co musí český zákon obsahovat (český zákonodárce může mít nad toto minimum další požadavky)
- Je potřeba mít na paměti, že z požadavku směrnice:
 - musí být regulovány všechny subjekty velikosti středního a velkého podniku (+ některé další) v daných odvětvích
 - musí zavádět bezpečnostní opatření podle čl. 20 a 21 směrnice apod.

Ve výsledku je ale podstatné především to, jak je směrnice převedena (transponována) do národního práva. Její samotný obsah má menší význam.

Návrh nového zákona o kybernetické bezpečnosti

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

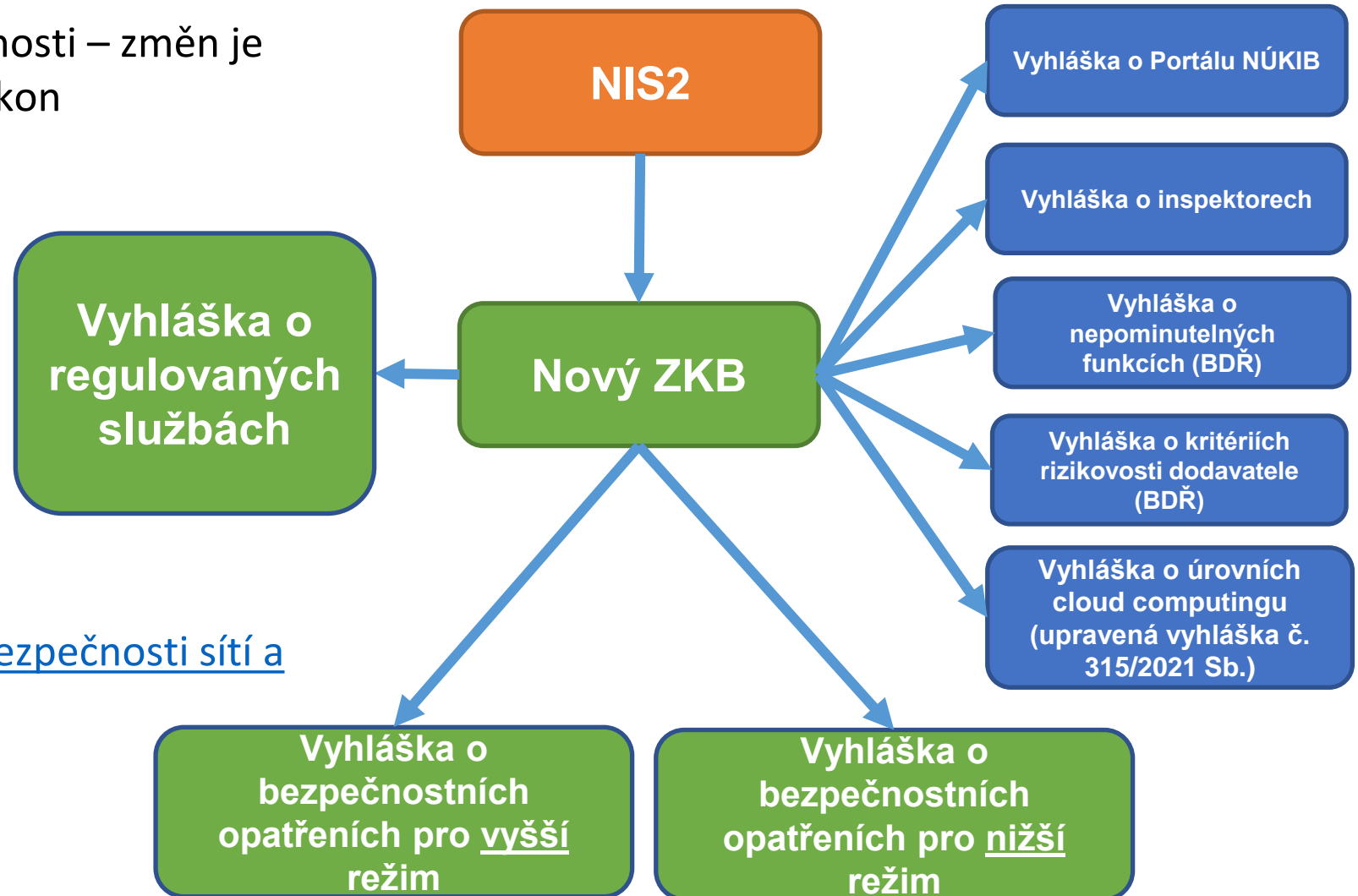
Nový zákon o kybernetické bezpečnosti (NZKB)



Nový zákon o kybernetické bezpečnosti – změna je tolik, že bylo třeba vytvořit nový zákon zcela nová úprava – cca 60 paragrafů

Zveřejněný návrh má aktuálně navíc 8 vyhlášek

Celý návrh zveřejněn zde: [Course: Nová směrnice EU o bezpečnosti sítí a informací \(nukib.cz\)](https://www.nukib.cz/course/nova-smernice-eu-o-bezpecnosti-siti-a-informaci)





- Dosavadní roztržitá struktura několika povinných osob se sdružuje do jedné – **poskytovatel regulované služby (PRS)** – *orientace podle IČO*
- **PRS je určován na základě kritérií ve vyhlášce o regulovaných službách (VoRS)**
- **Na základě kritérií je pro PRS určen režim regulace – vyšší nebo nižší**
- Kritéria jsou dvojí – pro identifikaci (vyhodnocuje adresát) a pro určení (vyhodnocuje NÚKIB)
- **Hlavní povinnosti**
 - **Hlásit údaje** – jak definuje Vyhláška o portálu NÚKIB
 - **Stanovit rozsah řízení kybernetické bezpečnosti** – definuje scope bezpečnosti
 - **Zavádět bezpečnostní opatření** – podle režimu v kterém je služba určena
 - **Hlásit kybernetické bezpečnostní incidenty**
 - **Informovat zákazníky o incidentech a hrozbách**
 - **Provádět protioopatření**
 - **Uplatnit pravidla lokalizace dat v případě vyššího režimu**
 - **Plnit povinnosti z Mechanismu řízení bezpečnosti dodavatelského řetězce**
 - **Podřídit se výkonu kontroly inspektorem v případě nižších povinností**
- Specifické situace – poskytování informací, stav kybernetického nebezpečí
- Úprava institucí – NÚKIB, CERT a jejich pravomoci
- Sankce – úprava horních limitů, změna přestupků

Jedna jediná povinná osoba*:

Poskytovatel regulované služby



Provozovatelé
základní služby

Kritická
(nejen informační)
infrastruktura

Významné
informační systémy

Všechny subjekty
z NIS2

*Pro primární sadu některých povinností spojených s prevencí – zavádění bezpečnostních opatření, hlášení incidentů, apod.



Režim vyšších povinností



Režim nižších povinností





- **Poskytovatel regulované služby**
 - Jediná povinná osoba
 - **Poskytuje regulovanou službu = služba splňující kritéria stanovená vyhláškou**
- **Režim poskytovatele regulované služby**
 - Stanovuje míru povinností – vyšší režim / nižší režim
 - Ke každému režimu bude vyhláška, která bude definovat povinnosti
- **Pokud bude jeden subjekt poskytovat služby v různých režimech – přednost má vyšší režim na všechny služby (tedy služby, které by byly v nižším režimu budou povýšeny do vyššího)**
- **Naplnění kritérií je povinen hlásit poskytovatel služby = každý si musí vyhodnotit kritéria sám**
 - Do 30 dnů od doby, kdy naplnění zjistí, nejpozději do 90 kdy k naplnění došlo
- **V případě naplnění kritérií se registruje u NÚKIB**
- **NÚKIB může zaregistrovat i sám dozvůli se o naplnění kritérií**



- Vše podle NIS2
- Nad rámec požadavků NIS2
 - Vybrané subjekty v odvětví letectví – po konzultaci s ÚCL
 - Vybrané subjekty v oblasti výzkumu a vývoje (nekomerční užití, veřejné financování, citlivá činnost, velké výzkumné infrastruktury)
 - Vojenský průmysl – vojenský materiál, zboží a technologie dvojího užití
 - Vybrané instituce veřejné správy



Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
1.1. Výkon svěřených pravomocí	<p>Orgán nebo osoba je</p> <p>I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je</p> <ul style="list-style-type: none"> a) ústředním orgánem státní správy, b) správním úřadem s celostátní působností, a to včetně ústředí a generálního ředitelství územně <u>dekoncentrovaných</u> (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Kanceláří Veřejného ochránce práv, g) Českou národní bankou, h) Nejvyšším kontrolním úřadem, i) Policejním prezidiem, j) útvarům policie s celostátní působností, k) orgánem soudní moci, l) státním zastupitelstvím, m) zdravotní pojišťovnou, n) krajem, o) hlavním městem Praha, nebo p) obcí s rozšířenou působností s nejméně 125 000 obyvateli,
	<p>II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je</p> <ul style="list-style-type: none"> a) územně <u>dekoncentrovaným</u> (specializovaným) orgánem státní správy, b) profesní komorou, c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností s počtem obyvatel do 125 000.



10. Vodní hospodářství

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
10.1. Provozování vodovodu	Provozovatel vodovodu podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) zásobuje pitnou vodou alespoň 50 000 obyvatel, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.
10.2. Provozování kanalizace	Provozovatel kanalizace podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) poskytuje služby odvádění nebo čištění odpadních vod alespoň 50 000 obyvatelům, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

18. Zdravotnictví

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
18.1. Poskytování zdravotní péče	Poskytovatel zdravotní péče podle zákona o zdravotních službách je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, b) disponuje počtem lůžek akutní péče nejméně 270, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

11. Odpadové hospodářství

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
11.1. Provoz zařízení určeného pro nakládání s odpady	Provozovatel zařízení určeného pro nakládání s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.2. Obchodování s odpadem	Obchodník s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.3. Zprostředkování nakládání s odpadem	Zprostředkovatel nakládání s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.4. Přeprava odpadu	Dopravce odpadu podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.

DEFINICE MALÉHO A STŘEDNÍHO PODNIKU

Při posuzování statutu malého a středního podniku (MSP) je nutné posuzovat i vztah k tzv. propojeným podnikům. Při výpočtech tak záleží na výši vlastnického podílu každého jednotlivého podniku, který má vlastnickou vazbu na zkoumaný podnik a naopak. Pro stanovení celkového počtu zaměstnanců, ročního obrátu či bilanční sumy roční rozvahy zkoumaného podniku se tak započítávají i údaje propojených podniků.

3 DRUHY PROPOJENÝCH PODNIKŮ

1. SAMOSTATNÝ PODNIK

Každý podnik, který vlastní méně než 25 % základního kapitálu nebo hlasovacích práv jiného podniku. **Údaje za tento podnik se nepřičítají.**

VÝJIMKY

Podnik se může považovat za nezávislý, a nemít tudíž žádné partnerské podniky, i tehdy, je-li 25% práh dosažen nebo překročen některým z investorů uvedených v doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

PŘÍKLADY VÝPOČTŮ

PŘÍKLAD 1

Posuzovaný podnik A je vlastněn ze 40 % podnikem B. K údajům za podnik A tedy přičítáme 40 % zaměstnanců a 40 % ročního obrátu a aktiv podniku B.

Výsledek = 100 % A + 40 % B



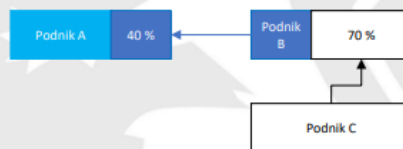
2. PARTNERSKÝ PODNIK

Každý podnik, který vlastní 25 % - 50 % základního kapitálu nebo hlasovacích práv jiného podniku. **Údaje za tento podnik se přičítají ve výši procentuálního vlastnického podílu.**

PŘÍKLAD 2

Posuzovaný podnik A je vlastněn ze 40 % podnikem B. Podnik B je navíc vlastněn podnikem C ze 70 %. Jelikož je mezi podnikem B a C spojenecký vztah, musíme k údajům za podnik A přičíst nejen 40 % zaměstnanců a 40 % ročního obrátu a aktiv podniku B, ale rovněž podniku C.

Výsledek = 100 % A + 40 % B + 40 % C



3. SPOJENÝ PODNIK

Každý podnik, který vlastní více než 50 % základního kapitálu nebo má právo uplatňovat rozhodující vliv v jiném podniku. **Údaje za tento podnik se přičítají v plné výši bez ohledu na procentuální vlastnický podíl.**

PŘÍKLAD 3

Posuzovaný podnik A vlastní z 51 % podnik B. K údajům za podnik A tedy přičítáme 100 % zaměstnanců a 100 % ročního obrátu a aktiv podniku B.

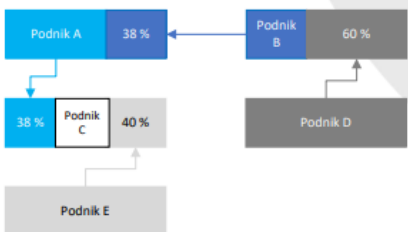
Výsledek = 100 % A + 100 % B



PŘÍKLAD 4

Posuzovaný podnik A je vlastněn z 38 % podnikem B. Zároveň podnik A vlastní 38 % podniku C. Podnik B je vlastněn podnikem D z 60 %, a podnik C je vlastněn podnikem E ve výši 40 %. K údajům za podnik A tedy přičítáme 38 % zaměstnanců a 38 % ročního obrátu a aktiv podniku B, dále 38 % z podniku C. Jelikož je podnik D ve spojeneckém vztahu k podniku B, musíme přičíst i 38 % z podniku D ve výši vlastněného podílu podniku B v posuzovaném podniku A. Údaje za podnik E nepřičítáme, protože se jedná o partnerský podnik námi vlastněného podniku C.

Výsledek = 100 % A + 38 % B + 38 % C + 38 % D



PŘÍKLAD 5

Posuzovaný podnik A je vlastněn z 60 % podnikem B. Podnik B má dva partnery, a to podnik C, který vlastní 32 % podniku B, a podnik D, který vlastní 25 % podniku B. K údajům za podnik A tedy přičítáme 100 % zaměstnanců a 100 % ročního obrátu a aktiv podniku B, dále 32 % podniku C, a 25 % podniku D.

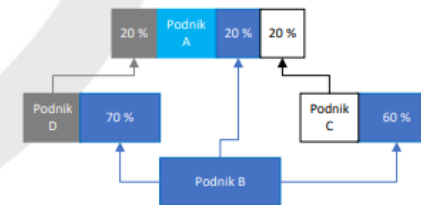
Výsledek = 100 % A + 100 % B + 32 % C + 25 % D



PŘÍKLAD 6

Posuzovaný podnik A je vlastněn podniky B, C a D, jejichž podíl je u každého roven 20 %. Při letném posouzení našeho vztahu k podnikům by se mohlo zdát, že se jedná o samostatný podnik, jelikož jednotlivé podíly nepřekračují hranici 25 %. Jelikož jsou ale podniky B, C a D vzájemnými spojenci, musíme jejich podíly na našem podniku A sečíst. Tím se dostáváme přes hranici 50% podílu na vlastnictví a všechny tři podniky se stávají našimi spojenci. Z toho vyplývá, že při výpočtu musíme přičíst údaje za celou skupinu.

Výsledek = 100 % A + 100 % B + 100 % C + 100 % D



Podrobnější výpočty a informace o tom, co vše započítat do velikosti zkoumaného podniku lze nalézt v uživatelské příručce k definici malých a středních podniků: https://osвета.nukib.cz/pluginfile.php/58365/mod_page/content/311/Priloha-4_U%C5%BElvatelsk%C3%A11%20p%C5%99%C3%ADru%C4%BDka%20k%20definici%20mal%C3%BDch%20a%20st%C5%99edn%C3%ADch%20podnik%C5%AF.pdf

verze 1.0, platná ke dni 14.11.2022



- rec. 16: „Má-li se zabránit tomu, aby subjekty, které mají partnerské podniky nebo které jsou přidruženými podniky, byly považovány za základní nebo důležité subjekty, kde by to bylo nepřiměřené, mohou členské státy při uplatňování čl. 6 odst. 2 přílohy doporučení 2003/361/ES zohlednit míru nezávislosti, v níž se subjekt ve vztahu ke svým partnerským nebo přidruženým podnikům nachází. Členské státy mohou zejména zohlednit skutečnost, že subjekt je na svém partnerovi nebo přidružených podnicích nezávislý z hlediska sítě a informačních systémů, které tento subjekt používá při poskytování svých služeb, a pokud jde o služby, které tento subjekt poskytuje. **Členské státy pak mohou mít v příslušném případě za to, že takový subjekt nesplňuje kritéria pro střední podnik podle článku 2 přílohy doporučení 2003/361/ES nebo nepřekračuje stropy pro střední podniky stanovené v odstavci 1 uvedeného článku, jestliže by se po zohlednění stupně nezávislosti uvedeného subjektu tento subjekt nepovažoval za subjekt, který je středním podnikem nebo za subjekt, který tyto stropy překračuje, pokud by se zohlednily pouze jeho vlastní údaje.** Povinnosti, které směrnice stanovuje partnerským a přidruženým podnikům, které do oblasti působnosti této směrnice spadají, zůstávají nedotčeny.“



Hlášení údajů

- Registrační údaje – info o organizaci
- Kontaktní údaje – info o zástupci, měl by být zastupitelný
- Doplnující údaje – IP rozsahy a další
- Potřeba hlásit i změny (těch údajů, které nelze dohledat v rejstřících)
- Náležitosti – vyhláška o Portálu NÚKIB

Stanovení rozsahu řízení bezpečnosti

- Identifikace primárních aktiv v rámci celé organizace
- Určí, která primární aktiva souvisí s poskytováním regulované služby
- Určí organizační části a podpůrná aktiva, která souvisí s poskytováním regulované služby
- **Ta aktiva a organizační části, která takto určí spadají do rozsahu regulace**
- Dokud/pokud to neudělá = rozsah celá organizace



Bezpečnostní opatření

- Zavádí se v rámci stanoveného rozsahu
- Začínají se plnit nejpozději do jednoho roku od registrace služby
- V rámci vyššího/nížšího režimu:

organizační opatření – vyšší režim

1. systém řízení bezpečnosti informací,
2. povinnosti pro vrcholné vedení,
3. bezpečnostní role,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. audit kybernetické bezpečnosti.

organizační opatření – nižší režim

1. zajišťování minimální úrovně kybernetické bezpečnosti,
2. povinnosti vrcholného vedení
3. bezpečnostní role
4. bezpečnostní politika a dokumentace,
5. řízení aktiv,
6. řízení dodavatelů,
7. bezpečnost lidských zdrojů,
8. řízení změn, akvizice, vývoje a údržby,
9. řízení přístupů,
10. zvládání kybernetických bezpečnostních událostí a incidentů,
11. řízení kontinuity činností.

technická opatření – vyšší režim (nižší režim mimo tučně vyznačené)

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
- 7. vyhodnocování kybernetických bezpečnostních událostí,**
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby,
11. zabezpečení průmyslových, řídicí a obdobných specifických aktiv.



Režim vyšších povinností

Hlásí vše
(s původem v kybernetickém prostoru)

Režim nižších povinností

**Hlásí incidenty s
významným dopadem**
(s původem v kybernetickém prostoru)

*významnost stanoví sám subjekt dle co nejjednoduššího postupu v prováděcím právním předpise



Opatření (nově Protiopatření)

- K podstatným změnám v logice opatření nedochází, mění se textace a některé detaily
- Nový institut – **Výstraha**
 - Jde o upozornění, které je veřejné, nezávazné
 - Vydává se z důvodu ochrany, pořádku, bezpečnosti, života a zdraví nebo ekonomiky
 - Muže být vydáno jako info o incidentu nebo o porušování ZKB
- **Varování** – o hrozbě nebo zranitelnosti – veřejné i neveřejné, musí se promítnout do analýzy rizik u vyššího režimu
- **Reaktivní protiopatření** – k řešení incidentu, zabezpečení před incidentem, ke zvýšení ochrany aktiv
 - Konkrétní úkony, technická opatření či postupy – pro adresáty povinné
 - Rozhodnutí – adresné (konkrétní adresát, konkrétní povinnost)
 - Opatření obecné povahy – neadresné (nekonkrétní adresát, konkrétní povinnost)



Řízení dodavatelů

- Povinnost poskytovatelů regulované služby **zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele** a požadavky dát do smluv
- Zohlednění bezpečnostních opatření není překážkou/omezením hospodářské soutěže podle ZZVZ
- **Předávání informací a dat od významného dodavatele** – Úřad může v případě hrozícího incidentu nařídit dodavateli předat data PRS ve vyšším režimu
 - Pouze na podnět, pokud hrozí incident, nutno doložit že standardní cestou to nešlo,
 - Úřad může určit formát, rozsah, způsob i termín předání



- Při stanovení úrovně zabezpečení a výběru konkrétních bezpečnostních opatření je potřeba v souladu se zákonem a vyhláškami **zohlednit specifika organizace a důležitost jednotlivých systémů a služeb** (není smyslem zavádět nesmyslná a nákladná řešení tam, kde to pro vaši organizaci nemá význam).
- Pokud vaše organizace kybernetickou bezpečnost do této chvíle systematicky neřešila, lze doporučit jako výchozí krok především **zmapování aktuálního stavu organizace** (tzn. audit aktuálního stavu kybernetické bezpečnosti a potenciálních slabých míst) a vypracováním **business impact analýzy** (zejm. jaké by byly dopady narušení řádného fungování jednotlivých systémů na vaši organizaci; nejde přitom jen o nedostupnost používaných informačních systémů, ale i o narušení důvěrnosti nebo integrity shromažďovaných dat).
- Již v této fázi je dobré se zaměřit na **školení relevantních osob** v organizaci – základní školení pro všechny uživatele, odborné školení pro osoby, které v organizaci řeší/budou řešit kybernetickou bezpečnost, nezapomínat přitom i na vrcholný management (management si musí být vědom důležitosti řízení kybernetické bezpečnosti v organizaci).
- **Rozhodně nedoporučujeme nakupovat služby typu „posoudíme soulad vaší organizace s NIS2“ nebo „zavedeme vám v organizaci NIS2“.** Nenechte se napálit „vševědoucími“ implementátory NIS2 na klíč. Směrnice NIS2 žádné konkrétní požadavky neupravuje, vše bude obsaženo až v novém zákoně o kybernetické bezpečnosti, který je teprve připravován.
- Z technických opatření lze obecně doporučit nasadit **firewally** (zejména perimetrové), **antiviry** (zejména sofistikovanější EDR), a **zálohovací řešení**. Společně s prováděním **aktualizací** (tam kde je to možné) se jedná o věci, které by měly být dávno běžnou součástí chodu každé organizace.



Děkuji za pozornost

Dotazy k návrhům nových předpisů je možné zasílat na:

regulace@nukib.cz